

## **Regulated Issuance of Digital Certificates**

### ***Abstract***

This invention allows a Certifying Authority (CA) in a Public Key Infrastructure (PKI) to allow a sub-CA to issue a pre-determined number of certificates without excessive overhead by the former CA. The regulation is performed by means of a security token that includes a count of the number of certificates issued by the sub-CA.

**REGULATED ISSUANCE OF DIGITAL CERTIFICATES**

Inventor/Applicant: **McKeon; Brian Bernard** (Sydney, NSW, Australia)

Date: 26/Jan/04

---

***References***

---

- [1] Digital Signatures, Atreya et al, RSA Press, 2002
- [2] MULTOS Smartcard Operating System, refer to MAOSCO Limited. St. Andrews House, The Links, Kelvin Close, Birchwood, Warrington, WA3 7PB. United Kingdom.
- [3] ISO7816-3, Identification Cards – Integrated Circuit(s) Cards with Contacts – Electronic Signals and Transmission Protocols
- [4] ISO7816-4, Identification Cards – Integrated Circuit(s) Cards with Contacts – Interindustry Commands for Interchange